

S. AMANDA MARSHALL, OSB #95347
United States Attorney
District of Oregon

DAVID L. ATKINSON, OSB #75021

Assistant United States Attorney
David.Atkinson@usdoj.gov
1000 SW Third Ave., Suite 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
Facsimile: (503) 727-1117

CHARLES F. GORDER, JR., OSB #912874

Assistant United States Attorney
Charles.Gorder@usdoj.gov
1000 SW Third Ave., Suite 600
Portland, OR 97204-2902
Telephone: (503) 727-1000
Facsimile: (503) 727-1117

ROBERT SANDER

Trial Attorney
Counterterrorism Section
National Security Division
United States Department of Justice
Attorneys for the United States of America

UNITED STATES DISTRICT COURT
DISTRICT OF OREGON
PORTLAND DIVISION

UNITED STATES OF AMERICA

Case No. 10-CR-506-KI

v.

**HOSSEIN LAHIJI and,
NAJMEH VAHID**

Defendants.

**GOVERNMENT'S UNCLASSIFIED
MEMORANDUM IN OPPOSITION
TO DEFENDANTS' MOTIONS TO
SUPPRESS AND MOTION FOR
CLASSIFIED MATERIALS**

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION
TO DEFENDANTS' MOTIONS TO SUPPRESS AND MOTION FOR CLASSIFIED
MATERIALS

TABLE OF CONTENTS

I.	SUMMARY OF CLASSIFIED, <i>EX PARTE</i> , FILING	2
II.	INTRODUCTION	2
	A. CLASSIFIED MATERIAL REDACTED	3
	B. Classified Materials Submitted to this Court	4
III.	THE FISA PROCESS	5
	A. Overview of the FISA Application Process	5
	1. The Certification	7
	2. Minimization Procedures	7
	3. Attorney General's Approval	8
	B. The FISC's Orders	9
IV.	THE COURT SHOULD UPHOLD THE FISA ORDERS HEREIN	12
	A. The FISA Orders Were Supported by Probable Cause	12
	1. The Standard of Review of Probable Cause	12
	2. The Instant FISA Applications Met FISA's Probable Cause Standard	14
	a. CLASSIFIED MATERIAL REDACTED	14
	b. CLASSIFIED MATERIAL REDACTED	14
	i. CLASSIFIED MATERIAL REDACTED	15
	ii. CLASSIFIED MATERIAL REDACTED	15

iii.	CLASSIFIED MATERIAL REDACTED	15
iv.	CLASSIFIED MATERIAL REDACTED	15
v.	CLASSIFIED MATERIAL REDACTED	15
3.	The FISC Correctly Concluded that the Targeted Facilities or Places were being Used, or were about to be Used by the Target of the Electronic Surveillance and that the Targeted Premises or Property were, or were about to be, Owned, Used, Possessed by, or were in Transit to or From, the Target of the Physical Searches	15
a.	CLASSIFIED MATERIAL REDACTED	15
b.	CLASSIFIED MATERIAL REDACTED	15
c.	CLASSIFIED MATERIAL REDACTED	15
d.	CLASSIFIED MATERIAL REDACTED	16
e.	CLASSIFIED MATERIAL REDACTED	16
B.	The Certifications Were Proper	16
1.	Standard of Review	16
2.	The Certifications Complied with FISA	17
a.	Foreign Intelligence Information	17
b.	A “Significant Purpose”	17
c.	Information Not Reasonably Obtainable Through Normal Investigative Techniques.....	17
C.	FISA is Subject to the “Good Faith” Exception	18
V.	THE FISA ORDERS WERE LAWFULLY EXECUTED	19

A.	The Standard Minimization Procedures	20
B.	The FISA Information Was Properly Minimized	25
C.	CLASSIFIED MATERIAL REDACTED	25
VI.	THE COURT’S REVIEW SHOULD ONLY BE CONDUCTED IN CAMERA AND EX PARTE	25
A.	The Court Must First Review the FISA Material Ex Parte and In Camera	25
B.	In Camera, Ex Parte Review is the Rule	27
C.	Nothing in the FISA Material Justifies a Departure from the General Rule of Ex Parte Examination Only	27
VII.	... THE COURT SHOULD REJECT THE DEFENDANTS’ ADDITIONAL LEGAL ARGUMENTS	31
A.	The Government Followed the Timing Requirements of FISA.....	31
B.	CLASSIFIED MATERIAL	32
C.	CLASSIFIED MATERIAL REDACTED	32
D.	The Significant Purpose Standard is Constitutional	32
VIII.	CONCLUSION	32

TABLE OF AUTHORITIES

I. CASES

- <i>ACLU Foundation of So. Cal. v. Barr</i> , 952 F.2d 457 (D.C. Cir. 1991).....	30
- <i>CIA v. Sims</i> , 471 U.S. 159 (1985).....	29
- <i>Halperin v. CIA</i> , 629 F.2d 144 (D.C. Cir. 1980)	29
- <i>In re Kevork</i> , 634 F. Supp. 1002 (C.D. Cal. 1985)	21, 28
- <i>In re Grand Jury Proceedings</i> , 347 F.3d 197 (7th Cir. 2003)	17
- <i>In re Sealed Case</i> , 310 F.3d 717 (FISA Ct. Rev. 2002)	13, 20
- <i>Massachusetts v. Sheppard</i> , 468 U.S. 981 (1984)	19
- <i>Phillippi v. CIA</i> , 655 F.2d 1325 (D.C. Cir. 1981).....	29
- <i>Scott v. United States</i> , 436 U.S. 128 (1978)	23
- <i>United States v. Abu-Jihaad</i> , 531 F. Supp. 2d 299 (D. Conn. 2008).....	27
- <i>United States v. Abu-Jihaad</i> , 630 F.3d 102 (2d Cir. 2010).....	12, 14, 26, 27
- <i>United States v. Ahmed</i> , No. 06-CR-147-WSD-CGB, 2009 U.S. Dist. Lexis 120007 (N.D. Ga. Mar. 19, 2009).....	12, 13 14
- <i>United States v. Alwan</i> , No. 1:11-CR-B-R, 2012 WL 5399154 (W.D.K.Y. Feb. 7 2012)	17
- <i>United States v. Badia</i> , 827 F.2d 1458 (11th Cir. 1987)	16, 17
- <i>United States v. Belfield</i> , 692 F.2d 141 (D.C. Cir. 1982)	27, 30
- <i>United States v. Bin Laden</i> , 126 F. Supp. 2d 264 (S.D.N.Y. 2000).....	20
- <i>United States v. Campa</i> 529 F.3d 980 (11th Cir. 2008)	16, 17
- <i>United States v. Canfield</i> , 212 F.3d 713 (2d Cir. 2000)	19
- <i>United States v. Cavanagh</i> , 807 F.2d 787 (9th Cir. 1987).....	13, 14
- <i>United States v. Crews</i> , 502 F.3d 1130 (9th Cir. 2007).....	12
- <i>United States v. Duggan</i> , 743 F.2d 59 (2d. Cir. 1984)	16, 18, 27

- <i>United States v. Duka</i> , 671 F.3d 329 (3rd Cir. 2011)	14, 18
- <i>United States v. El-Mezain</i> , 664 F.3d 467 (5th Cir. 2011)	14, 26, 27
- <i>United States v. Falcone</i> , 364 F. Supp. 877, 886 (D.N.J. 1973), <i>aff'd</i> , 500 F.2d 1401 (3rd Cir. 1974)	24
- <i>United States v. Garcia</i> , 413 F.3d 201 (2d Cir. 2005).....	17
- <i>United States v. Gourde</i> , 440 F.3d 1065 (9th Cir. 2006).....	12
- <i>United States v. U.S. Gypsum</i> , 333 U.S. 364 (1948)	17
- <i>United States v. Hammoud</i> , 381 F.3d 316 (4 th Cir. 2004)	13, 21, 23
- <i>United States v. Hammoud</i> , 405 F.3d 1054 (4th Cir. 2005).....	13
- <i>United States v. Hammoud</i> , 543 U.S. 1097 (2005)	13
- <i>United States v. Isa</i> , 923 F.2d 1300 (8th Cir. 1991)	23
- <i>United States v. Islamic Am. Relief Agency</i> , No. 07-00087-CR-W-NKL, 2009 WL 5169536 (W.D. Mo Dec. 1, 2009)	17, 23, 25, 26, 28
- <i>United States v. Kashmiri</i> , No. 09-CR-830-4, 2010 WL 4705159 (N.D. Ill., Nov. 10, 2010)	13, 26, 27
- <i>United States v. Leon</i> , 468 U.S. 897 (1984)	18
- <i>United States v. Mubayyid</i> , 521 F. Supp. 2d 125 (D.Mass 2007).....	21, 23, 31
- <i>United States v. Medunjanin</i> , No. 10-CR-19-1 (RJD), 2012 WL 526428 (S.D.N.Y.Feb. 16, 2012)	24
- <i>United States v. Nicholson</i> , No. 09-CR-40 (BR), 2010 WL 1641167 (D. Or. Apr. 21, 2010)	13, 16, 27
- <i>United States v. Ning Wen</i> , 477 F.3d 896 (7th Cir. 2007)	18, 19
- <i>United States v. Ott</i> , 827 F.2d 473 (9th Cir. 1987).....	28
- <i>United States v. Ott</i> , 637 F. Supp. 62 (E.D. Cal. 1986)	28

- <i>United States v. Rahman</i> , 861 F. Supp. 247 (S.D.N.Y. 1994).....	10, 20, 21
- <i>United States v. Rahman</i> , 189 F.3d 88 (2d Cir. 1999).....	11
- <i>United States v. Rosen</i> , 447 F. Supp. 2d 538 (E.D. Va. 2006)	10, 13, 16, 21, 25, 27
- <i>United States v. Salameh</i> , 152 F.3d 88 (2d Cir. 1998)	21
- <i>United States v. Sattar</i> , 395 F. Supp. 2d 79 (S.D.N.Y. 2005)	27
- <i>United States v. Sattar</i> , 590 F.3d 93 (2d Cir. 2009)	27
- <i>United States v. Sherifi</i> , 793 F. Supp. 2d 751 (E.D.N.C 2011).....	16, 25
- <i>United States v. Spanjol</i> , 720 F. Supp. 55 (E.D. Pa 1989)	27
- <i>United States v. Spanjol</i> , 958 F.2d 365 (3d Cir. 1992).....	27
- <i>United States v. Thomson</i> , 752 F. Supp. 75 (W.D.N.Y. 1990).....	21, 22, 27
- <i>United States v. United States District Court</i> , 407 U.S. 297 (1972)	14
- <i>United States v. Warsame</i> , 547 F. Supp. 2d 982 (D. Minn. 2008)	13, 16, 26, 28
- <i>United States v. Yunis</i> , 867 F.2d 617 (D.C. Cir. 1989).....	29

II. U.S. CONSTITUTION

Amend. I	10
Amend. IV	18, 32

III. FEDERAL STATUTES

Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1801:

-50 U.S.C. § 1801-1812	3
-50 U.S.C. § 1801(b).....	10
-50 U.S.C. § 1801(e)	7
-50 U.S.C. § 1801(h)(1)	8
-50 U.S.C. § 1801(h)(3)	8, 23
-50 U.S.C. § 1804(a)(1)-(9).....	6
-50 U.S.C. § 1804(a)(1)-(11).....	6
-50 U.S.C. § 1804(a)(6).....	17

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION
TO DEFENDANTS' MOTIONS TO SUPPRESS AND MOTION FOR CLASSIFIED
MATERIALS

-50 U.S.C. § 1804(a)(7).....	17
-50 U.S.C. § 1805(a)	11
-50 U.S.C. § 1805(a)(1)-(4).....	9
-50 U.S.C. § 1805(a)(2)(A)	10
-50 U.S.C. § 1805(a)(2)-(5).....	9
-50 U.S.C. § 1805(a)(3)(A)	10
-50 U.S.C. § 1805(a)(3)(B)	32
-50 U.S.C. § 1805(b)	11
-50 U.S.C. § 1805(c)(1)-(2).....	11
-50 U.S.C. § 1805(d)(1)	12
-50 U.S.C. § 1805(d)(2)	12
-50 U.S.C. § 1805(e)(1).....	11
-50 U.S.C. § 1805(e)(2).....	12
-50 U.S.C. § 1806(c)	3
50 U.S.C. § 1806(e)(2).....	20
-50 U.S.C. § 1806(f).....	26, 30
-50 U.S.C. § 1806(h)	33
-50 U.S.C. § 1821-1829	3
-50 U.S.C. § 1821(1).....	9, 10
-50 U.S.C. § 1821(4)(A)	8
-50 U.S.C. § 1821(4)(c).....	8, 23
-50 U.S.C. § 1823(a)(1)-(8).....	6
-50 U.S.C. § 1823(a)(1)-(9).....	6
-50 U.S.C. § 1823(a)(3)(B)-(C)	7
-50 U.S.C. § 1823(a)(4)(B)-(C)	7
-50 U.S.C. § 1823(a)(6).....	7
-50 U.S.C. § 1823(a)(7).....	7
-50 U.S.C. § 1824(a)	10
-50 U.S.C. § 1824(a)(1)-(4).....	9
-50 U.S.C. § 1824(a)(2)(A)	10

-50 U.S.C. § 1824(a)(2)-(5).....	9
-50 U.S.C. § 1824(a)(3)(A)	10
-50 U.S.C. § 1824(b)	11
-50 U.S.C. § 1824(c)(1)-(2).....	11
-50 U.S.C. § 1824(d)(1)	12
-50 U.S.C. § 1824(d)(2)	12
-50 U.S.C. § 1824(e)(1).....	12
-50 U.S.C. § 1824(e)(2).....	12
-50 U.S.C. § 1825(d)	3
-50 U.S.C. § 1825(f)(1)(B).....	20
-50 U.S.C. § 1825(g)	26

III. ORDERS, RULES, AND LEGISLATIVE AUTHORITIES

FED. R. CRIM. P. 41	13
H.R. Rep. No. 95-1283, 95th Cong., 2d Sess., Pt. 1 (1978)	21, 24
S. Rep. No. 95-701, 95th Cong., 2d Sess. (1978)	23

I. SUMMARY OF CLASSIFIED, *EX PARTE*, FILING

The defendants are charged in the District of Oregon in a two-count indictment with conspiracy to defraud the United States and conspiracy to transfer funds overseas to promote a violation of the sanctions imposed by the United States on U.S. persons doing business in Iran (hereafter the “Iranian embargo” or “Iranian sanctions”). In summary, the indictment alleges that the defendants laundered money through the Child Foundation which was operated by Mehrdad Yasrebi (“Yasrebi”) and located in Portland, Oregon. Yasrebi arranged to send the defendants’ funds to Iran where they were in part invested in real estate and bank accounts on the defendants’ behalf and provided to a radical ayatollah, all in violation of the Iranian embargo. The indictment also alleges that the defendants took inappropriate charitable deductions on their income tax for these personal investments and transfers to the ayatollah.

CLASSIFIED MATERIAL REDACTED

II. INTRODUCTION

The Government is filing this unclassified memorandum in opposition to “Defendant Najmeh Vahid’s Motion to Suppress with a Memorandum of Law in Support Thereof” (“Vahid Suppression Motion”) (CR 95, 105), “Defendant Najmeh Vahid’s Motion for Discovery of Classified Materials with Memorandum of Law in Support Thereof” (“Vahid Discovery Motion”) (CR 97), and Hossein Lahiji’s “Motion to Suppress” (CR 113) (collectively, “defendants’ motions”). Taken together, the defendants’ motions seek: (1) the disclosure of all applications, orders, and other related materials used to obtain warrants authorizing electronic surveillance and physical searches pursuant

to FISA;¹ and (2) the suppression of information obtained or derived from electronic surveillance, physical searches, or both, conducted pursuant to FISA that the Government will seek to introduce as evidence at trial.

CLASSIFIED MATERIAL REDACTED^{2,3}

A. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

On January 3, 2011, defendants Lahiji, Vahid, and this Court were provided with notice pursuant to 50 U.S.C. §§ 1806(c) and 1825(d) that the United States “intends to enter into evidence, use and disclose information acquired and derived from electronic surveillance . . . conducted pursuant to FISA, 50 U.S.C. §§ 1801-1811, and physical searches conducted pursuant to FISA, [50 U.S.C.] §§ 1821-1829.” (CR 6 at 1-2).

¹ **CLASSIFIED MATERIAL REDACTED**

² The provisions of FISA that address electronic surveillance are found at Title I of FISA (50 U.S.C. §§ 1801-1812); those that address physical searches are found at Title III (50 U.S.C. §§ 1821-1829). These two sets of provisions are in many respects parallel and almost identical. Citations herein are generally to the two sets of provisions in parallel, with the first citation being to the relevant electronic surveillance provision, and the second citation being to the relevant physical search provision. In addition, both Titles I and III have been amended since the authorized electronic surveillance and physical searches at issue. As a result, pertinent provisions of FISA have been renumbered, even when the substantive language remains identical. This Memorandum indicates where the current statutory language differs from that operative during the relevant time period in question.

³ This memorandum contains classified information from the relevant FISA materials. Accordingly, each paragraph and heading of this classified document is portion-marked. The letter or letters in parentheses at the beginning of each paragraph and section heading designate the relevant classification level. In accordance with Executive Order 13526, this memorandum is classified “SECRET,” which is the highest security classification level of any information contained herein. The letters “U” and “S” indicate that the information is, respectively, “UNCLASSIFIED” or is classified “SECRET.” The designations “ORCON” and “OC” (for “ORIGINATOR CONTROLLED”) indicate that this document may not be copied or otherwise used without the permission of the originator of the information. The designations “NOFORN” and “NF” (for “NO FOREIGN DISTRIBUTION”) indicate that this document may not be disseminated to non-United States persons.

B. Classified Materials Submitted to this Court**CLASSIFIED MATERIAL REDACTED⁴**

In subsequent sections of this Memorandum, the Government will: (1) discuss the FISA process; (2) present an overview of the specific FISA authorities at issue in this case; (3) summarize in detail the facts supporting the FISC's probable cause determinations with respect to the targets of the FISA-authorized electronic surveillance and physical searches and with respect to the facilities, places, premises, or property targeted (all of which information is contained fully in the exhibits in the Sealed Appendix); (4) discuss the certifications filed with the FISC; (5) discuss the relevant minimization procedures that were followed in this case; (6) address the manner in which the Court should conduct its *in camera, ex parte* review of the FISA materials; and (7) address the defendants' additional arguments in support of their various motions.

All of the Government's pleadings and supporting FISA materials are being submitted not only to oppose the defendants' motions, but also to support the United States' request, pursuant to FISA, that this Court: (1) conduct an *in camera, ex parte* review of the FISA materials; (2) find that the FISA information at issue was lawfully acquired and that the electronic surveillance and physical searches were made in conformity with an order of authorization or approval; and (3) order that none of the FISA materials, nor any of the classified information contained therein, be disclosed to the defense, and instead, that they be maintained by the United States under seal.

⁴ As a result of the redactions, the pagination and footnote numbering of the classified memorandum and the unclassified memorandum are different.

III. THE FISA PROCESS

A. Overview of the FISA Application Process

In its opinion and order in the case of *United States v. Mohamed Osman Mohamud*, No. 3:10-00475-KI (D. Or., CR 126, filed May 7, 2012) (attached as Unclassified Exhibit 1 and hereafter referred to as “*Mohamud*”), this Court described the structure of the FISC, the definition of “foreign intelligence information” under FISA, the process by which the government applies for a FISA order for electronic surveillance or physical search, the legal requirements which must be met in order for the FISC to issue such orders under FISA,⁵ and the necessary findings which must be accompany such orders. *Id.*, at pp. 3-7. In their memorandum in support of their motion to suppress (CR 105) at pages 3-8 the defendants do not contradict the Court’s description of FISA’s framework as set forth in *Mohamud*. In the interest of brevity, the government requests that the Court adopt that framework in addressing the defendants’ motions in this prosecution.

CLASSIFIED MATERIAL REDACTED

Under the version of FISA operative at the time of the applications in question, an application to conduct electronic surveillance pursuant to FISA must have contained, among other things:

- (1) the identity of the federal officer making the application;

⁵ **CLASSIFIED MATERIAL REDACTED**

- (2) the authority conferred on the Attorney General by the President of the United States and the approval of the Attorney General to make the application;
- (3) the identity, if known, or a description of the specific target of the electronic surveillance;
- (4) a statement of the facts and circumstances supporting probable cause to believe that the target is a foreign power or an agent of a foreign power, and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;
- (5) a statement of the proposed minimization procedures to be followed;
- (6) a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;
- (7) a certification, discussed below, of a high-ranking official;
- (8) the manner or means by which the electronic surveillance will be effected and a statement whether physical entry is required to effect the electronic surveillance;
- (9) the facts concerning and the action taken on all previous FISA applications involving any of the persons, facilities, or places specified in the application; and
- (10) the proposed duration of the electronic surveillance;
- (11) if the government intends to use more than one device, the coverage of the devices involved and the minimization procedures applicable to information acquired by each device.

50 U.S.C. § 1804(a)(1)-(11).⁶

An application to conduct a physical search pursuant to FISA must contain similar information as an application to conduct electronic surveillance. 50 U.S.C. § 1823(a)(1)-(9).⁷ The primary difference between the two sets of requirements is that an application to conduct a physical search must contain a statement of the facts and circumstances

⁶ Today, FISA imposes similar requirements as described by this Court in *Mohamud* at 5-6. See 50 U.S.C. § 1804(a)(1)-(9).

⁷ Today, FISA imposes similar requirements. See 50 U.S.C. § 1823(a)(1)-(8).

supporting probable cause to believe that “the premises or property to be searched contains foreign intelligence information” and that each “premises or property to be searched is owned, used, possessed by, or is in transit to or from” the target. 50 U.S.C. § 1823(a)(4)(B)-(C).⁸

1. The Certification

An application to the FISC for a FISA order must include a certification from a high-ranking executive branch official with national security responsibilities that:

- (A) the certifying official deems the information sought to be foreign intelligence information;
- (B) a significant purpose of the surveillance is to obtain foreign intelligence information;
- (C) such information cannot reasonably be obtained by normal investigative techniques;
- (D) designates the type of foreign intelligence information being sought according to the categories described in [50 U.S.C. §] 1801(e); and
- (E) including a statement of the basis for the certification that –
 - (i) the information sought is the type of foreign intelligence information designated; and
 - (ii) such information cannot reasonably be obtained by normal investigative techniques.

50 U.S.C. § 1804(a)(7); *see also* 50 U.S.C. § 1823(a)(7) (physical search).⁹

2. Minimization Procedures

The Attorney General has adopted, and the FISC has approved, minimization procedures that regulate the acquisition, retention, and dissemination of non-publicly

⁸ The same distinction continues today. *See* 50 U.S.C. § 1823(a)(3)(B)-(C).

⁹ Today, FISA imposes similar requirements. *See* 50 U.S.C. §§ 1804(a)(6), 1823(a)(6).

available information concerning unconsenting United States persons obtained through FISA-authorized electronic surveillance or physical searches, including persons who are not the targets of the FISA authorities. FISA requires that such minimization procedures be:

reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

50 U.S.C. § 1801(h)(1) (electronic surveillance); *see also* 50 U.S.C. § 1821(4)(A) (physical search).

In addition, minimization procedures also include “procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.” 50 U.S.C. § 1801(h)(3) (electronic surveillance; *see also* 50 U.S.C. § 1821(4)(c) (physical search).

In order to fulfill the statutory requirements discussed above, the Attorney General has adopted standard minimization procedures for FISA-authorized electronic surveillance and physical searches that are on file with the FISC and that are incorporated by reference into every FISA application that is submitted to the FISC and every order that is issued by the FISC. The FISC orders at issue here directed the Government to follow approved minimization procedures in conducting the electronic surveillance and physical searches.

3. Attorney General’s Approval

FISA further requires that the Attorney General approve applications for electronic surveillance, physical searches, or both, before they are presented to the FISC.

B. The FISC'S Orders

Once approved by the Attorney General, the application is submitted to the FISC and assigned to one of its judges. The FISC may approve the requested electronic surveillance, physical search, or both, only upon finding, among other things, that:

(1) the application has been made by a “Federal officer” and has been approved by the Attorney General;

(2) there is probable cause to believe that (a) the target of the electronic surveillance and/or physical search is a foreign power or an agent of a foreign power, and that (b) the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power (or that the premises or property to be searched is, or is about to be, owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power);

(3) the proposed minimization procedures meet the statutory requirements set forth in 50 U.S.C. § 1801(h) (electronic surveillance) and 50 U.S.C. § 1821(4) (physical search);

(4) the application contains all of the statements and certifications required by Section 1804 or Section 1823; and

(5) if the target is a United States person, that the certifications are not clearly erroneous.

50 U.S.C. §§ 1805(a)(2)-(5), 1824(a)(2)-(5).¹⁰

¹⁰ Today, FISA imposes similar requirements as described in *Mohamud* at 6-7. See 50 U.S.C. §§ 1805(a)(1)-(4), 1824(a)(1)-(4).

FISA defines “foreign power” to include, inter alia, “a foreign government or any component, thereof, whether or not recognized by the United States.” 50 U.S.C. §§ 1801(a), 1821(1).

“Agent of a foreign power” includes –

any person who –

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, which in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in [the subparagraphs above] . . . or knowingly conspires with any person to engage in activities described in [the subparagraphs above.]

50 U.S.C. §§ 1801(b), 1821(1).

FISA specifies that no United States person may be considered a foreign power or an agent of a foreign power solely on the basis of activities protected by the First Amendment to the Constitution of the United States. 50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A).¹¹ Although protected First Amendment activities cannot form the sole

¹¹ Today, FISA imposes similar requirements. *See* 50 U.S.C. §§ 1805(a)(2)(A), 1824(a)(2)(A).

basis for FISA-authorized electronic surveillance or physical searches, they may be considered by the FISC if there is other activity indicative that the target is an agent of a foreign power. *United States v. Rosen*, 447 F. Supp. 2d 538, 548 (E.D. Va. 2006) (noting probable cause determination may rely in part upon activities protected by the First Amendment, provided the determination also relies on activities not protected by the First Amendment”); *United States v. Rahman*, 861 F. Supp. 247, 252 (S.D.N.Y. 1994), *aff’d*, 189 F.3d 88 (2d Cir. 1999). Additionally, FISA provides that “[i]n determining whether or not probable cause exists . . . a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.” 50 U.S.C. §§ 1805(b), 1824(b).

If the FISC is satisfied that the FISA application meets the statutory provisions and has made all of the necessary findings, the FISC issues an *ex parte* order authorizing the electronic surveillance, physical searches, or both, requested in the application. 50 U.S.C. §§ 1805(a), 1824(a). The order must specify:

- (1) the identity (or a description of) the specific target of the collection;
- (2) the nature and location of each facility or place at which the electronic surveillance will be directed or of each of the premises or properties that will be searched;
- (3) the type of information sought to be acquired and the type of communications or activities that are to be subjected to the electronic surveillance, or the type of information, material, or property that is to be seized, altered, or reproduced through the physical search;
- (4) the manner and means by which electronic surveillance will be effected and whether physical entry will be necessary to effect that surveillance, or a statement of the manner in which the physical search will be conducted;
- (5) the period of time during which electronic surveillance is approved and/or the authorized scope of each physical search; and

(6) the applicable minimization procedures.

50 U.S.C. §§ 1805(c)(1)-(2), 1824(c)(1)-(2).

Under FISA, electronic surveillance or physical searches targeting a United States person may be approved for up to ninety days, and those targeting a non-United States person may be approved for up to one-hundred and twenty days. 50 U.S.C. §§ 1805(e)(1), 1824(e)(1).¹² Extensions may be granted, but only if the United States submits another application that complies with FISA's requirements. 50 U.S.C. §§ 1805(e)(2), 1824(e)(2).¹³ The duration of an extension for electronic surveillance or physical searches targeting a United States person may also be up to ninety days.

IV. THE COURT SHOULD UPHOLD THE FISA ORDERS AT ISSUE

A. The FISA Orders Were Supported by Probable Cause

1. Standard of Review of Probable Cause

Although federal courts are not in agreement as to whether the probable cause determinations of the FISC should be reviewed *de novo* or accorded due deference, the materials under review here pass muster under both standards. *See Abu-Jihaad*, 630 F.3d 102, 130 (2nd Cir. 2010) ("Although the established standard of judicial review applicable to FISA warrants is deferential, the government's detailed and complete submission in this case would easily allow it to clear a higher standard of review."). Understanding that the Ninth Circuit has not addressed the standard of review applicable in this matter and that this Court did not decide the issue in *Mohamud* at 13, the Government respectfully submits

¹² Today, FISA imposes similar requirements. *See* 50 U.S.C. §§ 1805(d)(1), 1824(d)(1).

¹³ Today, FISA imposes similar requirements. *See* 50 U.S.C. §§ 1805(d)(2), 1824(d)(2).

that it is appropriate to accord due deference to the findings of the FISC. Although in the minority, some courts, including the Second Circuit, have afforded due deference to the findings of the FISC. *Id.*; *see also United States v. Ahmed*, 2009 U.S. Dist. LEXIS 120007 (N.D. Ga. Mar. 19, 2009), at *21-22 (holding FISC’s “determination of probable cause should be given ‘great deference’ by the reviewing court” (citing *Illinois v. Gates*, 462 U.S. 213, 236 (1983))).

In the analogous area of criminal searches and surveillance, the law in the Ninth Circuit accords great deference to a magistrate judge’s probable cause determinations. *See, e.g., United States v. Crews*, 502 F.3d 1130, 1135 (9th Cir. 2007) (“A magistrate judge’s finding of probable cause is entitled to great deference....” (quoting *United States v. Clark*, 31 F.3d 831, 834 (9th Cir. 1994))); *see also United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006) (*en banc*) (noting court must not “flyspeck” the affidavit through *de novo* review). It would be consistent for a court that is reviewing FISA-authorized searches and surveillance to adopt the same posture it would when reviewing the probable cause determination of a criminal search warrant issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure. *See Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *21-22 (according FISC’s probable cause determinations the same deference as a magistrate’s criminal probable cause determination).¹⁴

¹⁴ *Ahmed* is not alone in analogizing FISA applications to criminal search warrants. *See e.g., United States v. Cavanagh*, 807 F.2d 787, 790 (9th Cir. 1987) (concluding that FISA order can be considered a warrant since it is issued by a detached judicial officer and is based on a reasonable showing of probable cause); *In Re Sealed Case*, 310 F.3d 717, 742 (FISC of Rev. 2002) (declining to decide whether a FISA order constitutes a warrant, but noting “that to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment”).

The Government notes, however, that a number of courts have declined to accord due deference to the findings of the FISC, citing the *ex parte* nature of the proceedings, and have instead reviewed the FISC's probable cause determination *de novo*.¹⁵ Despite the lack of agreement among federal courts as to whether the probable cause determinations of the FISC should be reviewed *de novo* or accorded due deference, the information provided to the FISC in support of the Government's applications for orders authorizing electronic surveillance and physical searches herein satisfies the higher standard of *de novo* review.

FISA requires a finding of probable cause that the target is a foreign power or an agent of a foreign power and that each facility or place at which the electronic surveillance is directed is being used, or is about to be used, or that property or premises to be searched is owned, used, possessed by, or is in transit to or from, a foreign power or an agent of a foreign power. It is this standard, not the standard applicable to criminal search warrants, which this Court must apply. *See United States v. El-Mezain*, 664 F.3d 467, 564 (5th Cir. 2011) ("This probable cause standard is different from the standard in the typical criminal case because, rather than focusing on probable cause to believe that a person has committed a crime, the FISA standard focuses on the status of the target as a foreign power or an agent of a foreign power."); *Abu-Jihaad*, 630 F.3d at 130-31; *United States v. Duka*, 671 F.3d 329, 338 (3rd Cir. 2011); *Cavanagh*, 807 F.2d. at 790 (citing *United States v.*

¹⁵ *See, e.g., United States v. Hammoud*, 381 F.3d 316, 332 (4th Cir. 2004), *rev'd on other grounds*, 543 U.S. 1097 (2005), *op. reinstated in pertinent part*, 405 F.3d 1034 (4th Cir. 2005); *Rosen*, 447 F. Supp. 2d at 545; *United States v. Warsame*, 547 F. Supp. 2d 982, 990-91 (D. Minn. 2008) (showing is "a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . , there is a fair probability" that the search will be fruitful (citing *Gates*, 462 U.S. at 238); *Kashmiri*, No. 09 CR 830-4, 2010 WL 4705159 (N.D. Ill., Nov. 10, 2010), at *1; *Nicholson*, No. 09-CR-40 (BR), 2010 WL 1641167 (D. Or., Apr. 21, 2010), *5. In each of these cases, the courts applied a *de novo* standard in reviewing the FISC's probable cause findings, and each court found that the applications before it contained probable cause.

United States District Court (Keith), 407 U.S. 297, 322 (1972)). This “different, and arguably lower, probable cause standard . . . reflects the purpose for which FISA search orders are issued.” *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *22.

2. The Instant FISA Applications Met FISA’s Probable Cause Standard

CLASSIFIED MATERIAL REDACTED

a. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

b. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

i. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

ii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iii. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

iv. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

v. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

3. The FISC Correctly Concluded that the Targeted Facilities or Places Were Being Used, or Were About to Be Used by the Target of the Electronic Surveillance and that the Targeted

**Premises or Property Were, or Were About to be, Owned,
Used, Possessed By, or were In Transit To or From,
the Target of the Physical Searches**

CLASSIFIED MATERIAL REDACTED

a. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

b. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

c. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

d. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

e. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

B. The Certifications Were Proper

1. Standard of Review

This Court correctly held in *Mohamud* that when the target of a FISA order is a United States person that the district court's review of the certifications are to ensure "that the certification or certifications are not clearly erroneous." *Mohamud* at 14.

Certifications submitted in support of a FISA application should be "subjected only to minimal scrutiny by the courts," *United States v. Badia*, 827 F.2d 1458, 1463 (11th Cir. 1987), and are "presumed valid." *United States v. Duggan*, 743 F.2d 59, 77 & n.6 (2nd. Cir.

1984) (citing *Franks v. Delaware*, 438 U.S. 154, 171 (1978)); *see also United States v.*

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION
TO DEFENDANTS' MOTIONS TO SUPPRESS AND MOTION FOR CLASSIFIED
MATERIALS

Campa, 529 F.3d 980, 993 (11th Cir. 2008) (quoting *Badia*); *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011) (noting “a presumption of validity [is] accorded to the certifications”); *Nicholson*, 2010 WL 1641167, at *5 (“[C]ertifications in the applications for FISA surveillance orders are ‘presumed valid.’ (quoting *Rosen*, 447 F. Supp. 2d at 545)); *Warsame*, 547 F. Supp. 2d at 990 (noting “a presumption of validity [is] accorded to the certifications”). When a FISA application is presented to the FISC, “[t]he FISA Judge, in reviewing the application, is not to second-guess the executive branch official’s certification that the objective of the surveillance is foreign intelligence information.” *Duggan*, 743 F.2d at 77. Likewise, Congress intended that the reviewing district court should “have no greater authority to second-guess the executive branch’s certifications than has the FISA judge.” *Id.*; see also *In re Grand Jury Proceedings*, 347 F.3d at 204-05; *Badia*, 827 F.2d at 1463; *Rahman*, 861 F. Supp. at 250; *United States v. Islamic Am. Relief Agency*, (“IARA”), No. 07-00087-CR-W-NKL, 2009 WL 5169536 (W.D. Mo., Dec. 21, 2009), at *4; *Kashmiri*, 2010 WL 4705159, at *1.

The district court’s review should determine whether the certifications were made in accordance with FISA’s requirements. See *United States v. Alwan*, No. 1:11-CR-13-R, 2012 WL 399154, at *7 (W.D. Ky. Feb. 7, 2012) (“‘The [c]ourt is not to second-guess whether the certifications were correct, but merely to ensure they were properly made.’” (quoting *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *20)); see also *Campa*, 529 F.3d at 993 (“[I]n the absence of a *prima facie* showing of a fraudulent statement by the certifying officer, procedural regularity is the only determination to be made if a non-United States person is the target.” (quoting *Badia*, 837 F.2d at 1463)). A certification is clearly

erroneous only when “the reviewing court on the [basis of the] entire evidence is left with

the definite and firm conviction that a mistake has been committed.” *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948); *see United States v. Garcia*, 413 F.3d 201, 222 (2d Cir. 2005); *IARA*, 2009 WL 5169536, at *4.

2. The Certifications Complied with FISA

CLASSIFIED MATERIAL REDACTED

a. Foreign Intelligence Information

CLASSIFIED MATERIAL REDACTED

b. A “Significant Purpose”

CLASSIFIED MATERIAL REDACTED

c. Information Not Reasonably Obtainable Through Normal Investigative Techniques

CLASSIFIED MATERIAL REDACTED

For all of the above reasons, the FISC correctly found that the certifications were not clearly erroneous.

C. FISA is Subject to the “Good-Faith” Exception

Finally, even assuming *arguendo* that this Court determines that a particular FISC order was not supported by probable cause, or that one or more of the FISA certification requirements were not in fact met, the Government respectfully submits that the evidence obtained or derived from the FISA-authorized electronic surveillance and physical searches is, nonetheless, admissible under the “good faith” exception to the exclusionary rule articulated in *United States v. Leon*, 468 U.S. 897 (1984).¹⁶ The Seventh Circuit, relying

¹⁶ “[E]ven if we were to conclude that amended FISA is unconstitutional, evidence derived from it would nevertheless have been admissible in the government’s case. . . . The exclusionary rule precludes the admission of evidence tainted by a Fourth Amendment violation” only in those cases
GOVERNMENT’S UNCLASSIFIED MEMORANDUM IN OPPOSITION
TO DEFENDANTS’ MOTIONS TO SUPPRESS AND MOTION FOR CLASSIFIED
MATERIALS

on *Leon*, held that federal officers were entitled to rely in good faith on a FISA warrant.

United States v. Ning Wen, 477 F.3d 896, 897 (7th Cir. 2007). As the court noted:

[T]he exclusionary rule must not be applied to evidence seized on the authority of a warrant, even if the warrant turns out to be defective, unless the affidavit supporting the warrant was false or misleading, or probable cause was so transparently missing that “no reasonably well trained officer [would] rely on the warrant.”

Id. (quoting *Leon*, 468 U.S. at 923) (alteration in original); *see also Duggan*, 743 F.2d at 77 n.6; *Ahmed*, 2009 U.S. Dist. LEXIS 120007, at *25 n.8, 26-27 (“The FISA evidence obtained . . . would be admissible under *Leon*’s ‘good faith’ exception to the exclusionary rule were it not otherwise admissible under a valid warrant.”).

The FISA-authorized electronic surveillance and physical searches at issue in this case would fall squarely within this “good faith exception.” First, there is no basis to find that any declarations or certifications at issue in this case were deliberately or recklessly false. *See Leon*, 468 U.S. at 914-15; *see also Massachusetts v. Sheppard*, 468 U.S. 981 (1984); *United States v. Canfield*, 212 F.3d 713, 717-18 (2d Cir. 2000). Further, there are no facts indicating that any of the independent Article III judges sitting as judges on the FISC failed to act in a neutral and detached manner in authorizing the surveillance and searches at issue. *Leon*, 468 U.S. at 914-15. Moreover, as the Court will see from its *in camera*, *ex parte* review of the FISA materials, facts establishing the requisite probable cause were submitted to the FISC, the FISC’s orders contained all of the requisite findings, and “well-trained officers” reasonably relied on those orders. *See Ning Wen*, 477 F.3d at 898. Therefore, in the event that the Court questions whether a particular FISC order was

where its application will deter police misconduct. *Duka*, 671 F.3d at 346, citing *Leon*, 468 U.S. at 918.

supported by sufficient probable cause, the information obtained pursuant to those orders would be admissible under *Leon's* “good faith” exception to the exclusionary rule.

V. THE FISA ORDERS WERE LAWFULLY EXECUTED

CLASSIFIED MATERIAL REDACTED¹⁷

This Court’s *in camera, ex parte* review of the FISA materials will demonstrate that the FISA surveillance and searches at issue were made in conformity with the orders of authorization or approval (“lawfully conducted”). That is, the FISA-obtained or -derived information at issue herein was acquired, retained, and disseminated by the FBI in accordance with FISA’s minimization requirements, and the SMPs adopted by the Attorney General and approved by the FISC.

A. The Standard Minimization Procedures

If a reviewing court is satisfied that the electronic surveillance or physical searches were properly certified and lawfully authorized pursuant to FISA, it must then examine whether the electronic surveillance or physical searches were lawfully conducted. *See* 50 U.S.C. §§ 1806(e)(2), 1825(f)(1)(B). In order to examine whether the electronic surveillance or physical searches were lawfully conducted, the reviewing court must determine whether the Government followed the relevant minimization procedures to appropriately minimize the information acquired pursuant to FISA.

CLASSIFIED MATERIAL REDACTED

FISA’s legislative history and the applicable case law demonstrate that the definitions of “minimization procedures” and “foreign intelligence information” were

¹⁷ *See* Sealed Exhibit 3, hereto.

intended to take into account the realities of collecting foreign intelligence because the activities of persons engaged in clandestine intelligence gathering or international terrorism are often not obvious on their face. *See Rahman*, 861 F. Supp. at 252-53. The degree to which information is required to be minimized varies somewhat given the specifics of a particular investigation, such that less minimization at acquisition is justified when “the investigation is focusing on what is thought to be a widespread conspiracy” and more extensive surveillance is necessary “to determine the precise scope of the enterprise.” *In re Sealed Case*, 310 F.3d at 741; *see also United States v. Bin Laden*, 126 F. Supp. 2d 264, 286 (S.D.N.Y. 2000) (“more extensive monitoring and greater leeway in minimization efforts are permitted in a case like this given the world-wide, covert and diffuse nature of the international terrorist group(s) targeted” (internal quotation marks omitted)).

Furthermore, the activities of foreign powers and their agents are often not obvious from an initial or cursory overhear of conversations. To the contrary, agents of foreign powers frequently engage in coded communications, compartmentalized operations, the use of false identities and other practices designed to conceal the breadth and aim of their operations, organization, activities and plans. *See, e.g., United States v. Salameh*, 152 F.3d 88, 154 (2d Cir. 1998) (noting that two conspirators involved in the 1993 bombing of the World Trade Center in New York referred to the bomb plot as the “study” and to terrorist materials as “university papers”). As one court explained, “[i]nnocuous-sounding conversations may in fact be signals of important activity; information on its face innocent when analyzed or considered with other information may become critical.” *Kevoork*, 634 F. Supp. at 1017 (quoting H.R. Rep. No. 95-1283, pt. I (1978) (hereinafter “House Report”)); *see also Hammoud*, 381 F.3d at 334 (citing *Salameh*, 152 F.3d at 154); *In re Sealed Case*,

310 F.3d at 740-41; *United States v. Thomson*, 752 F. Supp. 75, 81 (W.D. N.Y. 1990) (noting that it is permissible to retain and disseminate “bits and pieces” of information until the information’s “full significance becomes apparent”) (citing House Report, part 1, at 58); *Bin Laden*, 126 F. Supp. 2d at 286. Likewise, “individual items of information, not apparently significant when taken in isolation, may become highly significant when considered together over time.” *Rahman*, 861 F. Supp. at 252-53 (citing House Report, part 1, at 55, 59). The Government must be given flexibility where the conversations are carried out in a foreign language. *United States v. Mubayyid*, 521 F. Supp. 2d 125, 134 (D. Mass. 2007); *Rahman*, 861 F. Supp. at 252. As a result, “courts have construed ‘foreign intelligence information’ broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information.” *Rosen*, 447 F. Supp. 2d at 551.

The nature of the foreign intelligence information sought also impacts implementation of the minimization procedures at the retention and dissemination stages. There is a legitimate need to conduct a thorough post-acquisition review of FISA information that involves a U.S. person who is acting as an agent of a foreign power. Congress explained:

It is “necessary” to identify anyone working with him in this network, feeding him information, or to whom he reports. Therefore, it is necessary to acquire, retain and disseminate information concerning all his contacts and acquaintances and his movements. Among his contacts and acquaintances, however, there are likely to be a large number of innocent persons. Yet, information concerning these persons must be retained at least until it is determined that they are not involved in the clandestine intelligence activities and may have to be disseminated in order to determine their innocence.

House Report, part 1, at 58. Indeed, at least one court has cautioned that, when a U.S. person communicates with an agent of a foreign power, the Government would be “remiss

in meeting its foreign counterintelligence responsibilities” if it did not thoroughly “investigate such contacts and gather information to determine the nature of those activities.” *Thomson*, 752 F. Supp. at 82.

Congress also recognized that agents of a foreign power are often very sophisticated and skilled at hiding their activities. *Cf. Thomson*, 752 F. Supp. at 81 (quoting House Report part 1, at 58). Accordingly, to pursue leads, Congress intended that the Government be given “a significant degree of latitude” with respect to the “retention of information and the dissemination of information between and among counterintelligence components of the Government.” *Cf. Thomson*, 752 F. Supp. at 81 (quoting House Report part 1, at 58).

In light of these realities, Congress recognized that “no electronic surveillance can be so conducted that innocent conversations can be totally eliminated.” *See* S. Rep. No. 95-701, 95th Cong., 2d Sess., 39 (quoting *Keith*, 407 U.S. at 323) (1978) (“Senate Report”). The Fourth Circuit reached the same conclusion in *Hammoud*, stating that the “mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance.” 381 F.3d at 334.

Accordingly, in reviewing the adequacy of minimization efforts, the test to be applied is neither whether innocent conversations were intercepted, nor whether mistakes were made with respect to particular communications. Rather, as the United States Supreme Court stated in the context of Title III surveillance, there should be an “objective assessment of the [agents’] actions in light of the facts and circumstances confronting [them] at the time.” *Scott v. United States*, 436 U.S. 128, 136 (1978). “The test of compliance is ‘whether a good faith effort to minimize was made.’” *Mubayyid*, 521 F.

Supp. 2d at 135. *See also Hammoud*, 381 F.3d at 334 (“[t]he minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information”); *see also* Senate Report at 39-40 (stating that the court’s role is to determine whether “on the whole, the agents have shown a high regard for the right of privacy and have done all they reasonably could do to avoid unnecessary intrusion”); *IARA*, 2009 WL 5169536, at *6 (quoting Senate Report at 39-40).

Moreover, as noted above, FISA expressly states that the Government is not required to minimize information that is “evidence of a crime,” whether or not it is also foreign intelligence information. 50 U.S.C. §§ 1801(h)(3), 1821(4)(c); *see also Isa*, 923 F.2d at 1304 (upholding district court’s denial of adversarial hearing) (noting that “[t]here is no requirement that the ‘crime’ be related to foreign intelligence”). As a result, to the extent that certain communications of a U.S. person may be evidence of a crime or otherwise may establish an element of a substantive or conspiratorial offense, such communications need not be minimized. *See Id.* at 1305.

Even assuming, *arguendo*, that certain communications were not properly minimized, suppression is not the appropriate remedy with respect to the communications that met the standard. *Cf. United States v. Falcone*, 364 F. Supp. 877, 886-87 (D.N.J. 1973), *aff’d*, 500 F.2d 1401 (3d Cir. 1974) (Title III). As discussed above, absent evidence that “on the whole” there has been a “complete” disregard for the minimization procedures, the fact that a court might conclude that some communications should have been minimized does not affect the admissibility of items properly acquired and retained. Indeed, Congress specifically intended that the only evidence that should be suppressed is

the “evidence which was obtained unlawfully.” House Report at 93. FISA’s legislative history reflects that Congress intended only a limited sanction for errors of minimization:

As the language of the bill makes clear, only that evidence which was obtained unlawfully or derived from information obtained unlawfully would be suppressed. If, for example, some information should have been minimized but was not, only that information should be suppressed; the other information obtained lawfully should not be suppressed.

Id.; see also *Falcone*, 364 F. Supp. at 886-87.

Indeed, courts have held that minor deviations do not warrant disclosure, adversarial hearings, or suppression of all evidence collected pursuant to electronic surveillance. See, e.g., *United States v. Medunjanin*, No. 10 CR 19 1(RJD), 2012 WL 526428, at *12 (S.D.N.Y. Feb. 16, 2012) (finding that disclosure and suppression were unwarranted when “any failure to adhere to [minimization] protocol was *de minimis*” and “the consequences were equally negligible”). Courts have denied defendants’ motions to suppress and for disclosure when any failure to minimize was “(i) inadvertent, (ii) disclosed to the FISC upon discovery, and (iii) promptly rectified.” *Rosen*, 447 F. Supp. 2d at 552; see also *United States v. Sherifi*, 793 F. Supp. 2d 751, 760 (E.D.N.C. 2011) (“Any failure to minimize was inadvertent, disclosed to the FISC upon discovery, and promptly rectified.”); *IARA*, 2009 WL 5169536, at *6 (quoting *Rosen*).

B. The FISA Information Was Properly Minimized

CLASSIFIED MATERIAL REDACTED

C. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

**VI. THE COURT’S REVIEW SHOULD ONLY BE CONDUCTED
IN CAMERA AND EX PARTE**

GOVERNMENT’S UNCLASSIFIED MEMORANDUM IN OPPOSITION
TO DEFENDANTS’ MOTIONS TO SUPPRESS AND MOTION FOR CLASSIFIED
MATERIALS

In light of the above discussion demonstrating that the FISA surveillance and searches in this matter were lawfully authorized and properly executed, the Court's *in camera* and *ex parte* review of the FISA materials is sufficient and the defendants' motions for access to those classified materials should be denied.

A. The Court Must First Review the FISA Material *Ex Parte* and *In Camera*

In assessing the legality of FISA-authorized electronic surveillance, physical searches, or both, the district court, "shall, notwithstanding any other law, if the Attorney General files [as he has filed in this proceeding] an affidavit or declaration under oath that disclosure or an adversary hearing would harm the national security of the United States, review *in camera* and *ex parte* the application, order, and such other materials relating to the surveillance [or physical search] as may be necessary to determine whether the surveillance [or physical search] of the aggrieved person was lawfully authorized and conducted."¹⁸ 50 U.S.C. §§ 1806(f), 1825(g). On the filing of the Attorney General's affidavit or declaration, the court "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance [or physical search] *only where such disclosure is necessary* to make an accurate determination of the legality of the surveillance [or search]."¹⁹ 50 U.S.C. §§ 1806(f), 1825(g) (emphasis added). Thus, the propriety of the disclosure of any FISA applications or orders to the defense cannot even be considered

¹⁸ **CLASSIFIED MATERIAL REDACTED**

¹⁹ In *Warsame*, the court addressed the meaning of "necessary" in this context, noting that "[t]he legislative history explains that such disclosure is 'necessary' only where the court's initial review indicates that the question of legality may be complicated" by factual misrepresentations, insufficient identification of the target, or failure to comply with the minimization standards in the order. 547 F. Supp. 2d at.

unless and until the district court has first concluded that it is unable to make an accurate determination of the legality of the collection after reviewing the Government's submissions (and any supplemental pleadings that the district court may request) *in camera* and *ex parte*. See *El-Mezain*, 664 F.3d at 565; *Abu-Jihaad*, 630 F.3d at 129; *Nicholson*, 2010 WL 1641167, at *4 (“After an *in-camera* review, the court ‘has the discretion to disclose portions of the documents, under appropriate protective procedures, *only if [the court] decides that such disclosure is necessary to make an accurate determination of the legality of the surveillance.*’” (quoting *Duggan*, 743 F.2d at 78)); *Kashmiri*, 2010 WL 4705159, at *2 (quoting *Duggan*); *IARA*, 2009 WL 5169536, at *3-4.

If the district court is able to make an accurate determination of the legality of the electronic surveillance or physical searches based on its *in camera*, *ex parte* review of the materials submitted by the United States, then the court *may not* order disclosure of any of the FISA materials to the defense, unless otherwise required by due process. *El-Mezain*, 664 F.3d at 566; *Abu-Jihaad*, 630 F.3d at 129; *Duggan*, 743 F.2d at 78; *Kashmiri*, 2010 WL 4705159, at *2. This Court has previously ruled that this *ex parte* procedure is constitutional. *Mohamud* at 11-12.

B. *In Camera*, *Ex Parte* Review is the Rule

Federal courts have repeatedly and consistently held that FISA “anticipates that an *ex parte*, *in camera* determination is to be the rule,” with disclosure and an adversarial hearing being the “exception, occurring *only* when necessary.” *United States v. Belfield*, 692 F.2d 141, 147 (D.C. Cir. 1982) (emphasis in original); see also *El-Mezain*, 664 F.3d at 567 (“[D]isclosure of FISA materials ‘is the exception and *ex parte*, *in camera* determination is the rule.’” (quoting *United States v. Stewart*, 590 F.3d 93, 129 (2d Cir.

2009)); *Duggan*, 743 F.2d at 78; *Nicholson*, 2010 WL 1641167, at *3-4; *Rosen*, 447 F. Supp. 2d at 546; *United States v. Spanjol*, 720 F. Supp. 55, 59 (E.D. Pa. 1989), *aff'd*, 958 F.2d 365 (3d Cir. 1992) (“It is well established that the legality of foreign intelligence surveillance should be determined on an *in camera*, *ex parte* basis.”).

In fact, as this Court has previously noted, every court that has addressed a motion to disclose FISA materials or to suppress FISA information has been able to reach a conclusion as to the legality of the FISA collection at issue based on its *in camera*, *ex parte* review. *Mohamud* at 9.

C. Nothing in the FISA Materials Justifies a Departure from the General Rule of *Ex Parte* Examination Only

As the Court will see from its examination of the exhibits in the Sealed Appendix, there is nothing that extraordinary about the instant FISA-authorized electronic surveillance and physical searches that would justify this case becoming the first “exception” to the rule of all previous FISA litigation – that is, the first-ever to order the production and disclosure of highly sensitive and classified FISA materials or the suppression of FISA-obtained or -derived evidence. Here, the FISA materials are well-organized and easily reviewable by the Court *in camera* and *ex parte*, and they are fully and facially sufficient to allow the Court to make an accurate determination that the FISA information was lawfully acquired and that the surveillance and searches were made in conformity with an order of authorization or approval. The instant materials “are straightforward and readily understood.” *Kevork*, 634 F. Supp. at 1008. Moreover, as in other cases, “[t]he determination of legality in this case is not complex.” *Belfield*, 692 F.2d at 147; *see also Warsame*, 547 F. Supp. 2d at, 987 (“[T]he issues presented by the FISA

applications are straightforward and uncontroversial”); *Abu-Jihaad*, 531 F. Supp. 2d at 310; *Thomson*, 752 F. Supp. at 79. The Government respectfully submits that, as it was in the *Mohamud* case, this Court is capable of reviewing the FISA materials *in camera* and *ex parte* and making the requisite legal determination without an adversarial hearing.

CLASSIFIED MATERIAL REDACTED

“In the sensitive area of foreign intelligence gathering, the need for extreme caution and sometimes even secrecy may not be overemphasized.” *United States v. Ott*, 637 F. Supp. 62, 65 (E.D. Cal. 1986); see also *United States v. Ott*, 827 F.2d 473, 477 (9th Cir. 1987) (“Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to anyone not involved in the surveillance operation in question”); IARA, 2009 WL 5169536, at *3-4 (quoting *Ott* District Court opinion).

Confidentiality is critical to national security. “If potentially valuable intelligence sources” believe that the United States “will be unable to maintain the confidentiality of its relationship to them, many [of those sources] could well refuse to supply information.” *C.I.A. v. Sims*, 471 U.S. 159, 175 (1985); see also *Phillippi v. CIA*, 655 F.2d 1325, 1332-33 (D.C. Cir. 1981). When a question is raised as to whether the disclosure of classified sources, methods, techniques, or information would harm the national security, federal courts have expressed a great reluctance to replace the considered judgment of Executive Branch officials charged with the responsibility of weighing a variety of subtle and complex factors in determining whether the disclosure of information may lead to an unacceptable risk of compromising the intelligence gathering process, and determining

whether foreign agents, spies, and terrorists are capable of piecing together a mosaic of

GOVERNMENT’S UNCLASSIFIED MEMORANDUM IN OPPOSITION
TO DEFENDANTS’ MOTIONS TO SUPPRESS AND MOTION FOR CLASSIFIED
MATERIALS

information that, when revealed, could reasonably be expected to harm the national security of the United States. *See Sims*, 471 U.S. at 180; *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) (“Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation’s intelligence-gathering capabilities from what these documents revealed about sources and methods.”); *Halperin v. CIA*, 629 F.2d 144, 150 (D.C. Cir. 1980) (“[E]ach individual piece of intelligence information, much like a piece of jigsaw puzzle, may aid in piecing together other bits of information even when the individual piece is not of obvious importance in itself.”). An adversary hearing is not only unnecessary to aid the Court in the straightforward task before it, but such a hearing would *create* potential dangers that courts have consistently sought to avoid.

As the *Belfield* court explained:

Congress recognized the need for the Executive to engage in and employ the fruits of clandestine surveillance without being constantly hamstrung by disclosure requirements. The statute is meant to “reconcile national intelligence and counterintelligence needs with constitutional principles in a way that is consistent with both national security and individual rights.” In FISA the privacy rights of individuals are ensured not through mandatory disclosure, but through its provisions for in-depth oversight of FISA surveillance by all three branches of government and by a statutory scheme that to a large degree centers on an expanded conception of minimization that differs from that which governs law enforcement surveillance.

692 F.2d at 148 (footnotes and citations omitted); *see also ACLU Found. of So. Cal. v.*

Barr (“*ACLU Foundation*”), 952 F.2d 457, 465 (D.C. Cir. 1991) (citing *Belfield* for the proposition that Section 1806(f) “is an acceptable means of adjudicating the constitutional rights of persons who have been subjected to FISA surveillance”).

GOVERNMENT’S UNCLASSIFIED MEMORANDUM IN OPPOSITION
TO DEFENDANTS’ MOTIONS TO SUPPRESS AND MOTION FOR CLASSIFIED
MATERIALS

In this case, the defendants have not presented any reason to believe that any FISA application contains any falsehoods or omissions, that the applicable minimization procedures were inadequate or that the Government failed to comply with them, or that the requisite certifications were either not made or were clearly erroneous. Nor can the defendants' lack of access to any FISA application or order form a substitute basis for the Court to order disclosure. Despite the quandary defense counsel inevitably face when notified that FISA-obtained or -derived information will be used against a defendant, Congress mandated, and the courts have recognized, that this quandary does not justify the disclosure of FISA materials:

We appreciate the difficulties of appellants' counsel in this case. They must argue that the determination of legality is so complex that an adversary hearing with full access to relevant materials is necessary. But without access to relevant materials their claim of complexity can be given no concreteness. It is pure assertion.

Congress was also aware of these difficulties. But it chose to resolve them through means other than mandatory disclosure. In FISA Congress has made a thoroughly reasonable attempt to balance the competing concerns of individual privacy and foreign intelligence Appellants are understandably reluctant to be excluded from the process whereby the legality of a surveillance by which they were incidentally affected is judged. But it cannot be said that this exclusion rises to the level of a constitutional violation.

Belfield, 692 F.2d at 148. *See also Mubayyid*, 521 F. Supp. 2d at 131. For all of these reasons, the defendants' motions for access to the classified material should be denied.

VII. THE COURT SHOULD REJECT THE DEFENDANTS' ADDITIONAL LEGAL ARGUMENTS

The remaining motions of the defendants can be disposed of expeditiously. The Vahid Suppression Motion, in which defendant Lahiji joins, claims without further support or elaboration that "the Government failed to satisfy the significant purpose, probable

GOVERNMENT'S UNCLASSIFIED MEMORANDUM IN OPPOSITION
TO DEFENDANTS' MOTIONS TO SUPPRESS AND MOTION FOR CLASSIFIED
MATERIALS

cause, certification, minimization, and timing requirements of FISA.”²⁰ (Doc. 95 at 3).

Those arguments are primarily addressed and rebutted above.

A. The Government Followed the Timing Requirements of FISA

The Government is at a disadvantage in attempting to reply to the defendants’ vague statement that “the Government failed to satisfy the . . . timing requirement[] of FISA.” (Doc. 105 [memorandum of law in support of Doc. 95] at 3.) A particular FISA collection may be extended or renewed for additional periods of time upon the presentation to the FISC of another application that satisfies all of FISA’s requirements. To the extent that the defendants are speculating that a FISC order was for a greater period of time than that authorized by FISA or whether there was unauthorized collection beyond any FISC-authorized time frame, the Government submits that the Court’s *in camera, ex parte* review of the FISA materials will dispel any such contention.

B. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED

C. CLASSIFIED MATERIAL REDACTED

CLASSIFIED MATERIAL REDACTED²¹

D. The Significant Purpose Standard is Constitutional

Finally, defendant Lahiji additionally argues that the current “significant purpose” requirement of FISA is unconstitutional and that FISA surveillance is only consistent with

²⁰ There are two other vague allegations relating to minimization in the Vahid Suppression Motion: an allegation that “[i]t is evident that the Government failed to comply with FISA’s minimization requirements and procedure” (Doc. 95 at 8); and an allegation that “there certainly appears to be an issue, at the least, with minimization standards utilized.” (Doc. 95 at 9).

²¹ At CR 113 at p. 2, where the provision is erroneously cited as 50 U.S.C. § 1805(a)(4).

the Fourth Amendment if foreign intelligence collection is its “primary purpose.” CR 113 at 2. This Court found to the contrary in *Mohamud* and based upon the analysis set forth therein should reject that argument here. *Mohamud* at 9-11.

VIII. CONCLUSION

The defendants’ motions should all be denied. Based on the foregoing analysis, the Government respectfully submits that the Court should: (1) conduct an *in camera*, *ex parte* review of the FISA materials and the Government’s classified submission; (2) find that the FISA surveillance was lawfully authorized and lawfully conducted in compliance with the Fourth Amendment; (3) hold that disclosure of the FISA materials and the Government’s classified submissions to the defense is not required because the Court is able to make an accurate determination of the legality of the surveillance without disclosing the FISA materials or any portions thereof; (4) order that the FISA materials and the Government’s classified submissions be maintained under seal by the Classified Information Security Officer or his/her designee; and (5) deny each of the defendants’ pending motions to suppress and obtain access to the FISA materials in this matter.²²

DATED: January 9, 2013

Respectfully submitted,

S. AMANDA MARSHALL

²² A district court order granting motions or requests under 50 U.S.C. § 1806(g), a decision that electronic surveillance was not lawfully authorized or conducted, and an order requiring the disclosure of FISA materials is a final order for purposes of appeal. 50 U.S.C. § 1806(h). In the unlikely event that the Court concludes that disclosure of any item within any of the FISA materials or suppression of any FISA-obtained or -derived information may be required, given the significant national security consequences that would result from such disclosure or suppression, the Government would expect to pursue an appeal. Accordingly, the Government respectfully requests that the Court indicate its intent to do so before issuing any order, and that the Court stay any such order pending an appeal by the United States of that order.

United States Attorney

DAVID L. ATKINSON
CHARLES F. GORDER, JR.
Assistant United States Attorneys

Attorneys for Plaintiff
UNITED STATES OF AMERICA